IN THE CLAIMS:

Claims 1, 2, 6, 7, 8, 13, 17, 18, 21, 24, 25, 27 are amended herein. Claims 11 and 12 are cancelled. All pending claims and their present status are produced below.

1. (Currently amended) A method for use in analyzing network security, comprising:

constructing query-based rules ~~to be used to identify network conditions~~ for determining the presence of a set of conditions in at least one network resource, wherein the set of conditions collectively define known network security properties of the at least one network resource in which the set of conditions are present.

2. (Currently amended) The method of claim 1, wherein known network security properties ~~conditions~~ include vulnerability network security properties ~~conditions~~ and intrusion network security properties ~~conditions~~.

3. (Original) The method of claim 1, wherein the step of constructing query-based rules includes constructing query-based rules from a set of lexical elements that includes a set of templates.

4. (Original) The method of claim 3, wherein the templates are divided into two classes comprising template types and template actions.

5. (Original) The method of claim 1, wherein the step of constructing query-based rules includes constructing query-based rules from a set of lexical elements that includes a set of statements, a set of templates, and a set of reserved words.

6. (Currently amended) The method of claim 5, wherein:

known network security properties ~~conditions~~ include vulnerability network security properties ~~conditions~~ and intrusion network security properties ~~conditions~~;

the set of statements includes SET and SELECT;

the set of reserved words includes AND, TO, and WHERE; and

the set of templates includes:

a first subset of templates, the first subset of templates for determining the presence of ~~identifying network vulnerability~~ conditions that collectively define known vulnerability network security properties, wherein the first subset comprises:

Operating System, Host, Protocol, Application, Vulnerability, Port, Execute, ExecuteHex, Contains, and ContainsHex;

a second subset of templates, the second subset of templates for determining the presence of ~~identifying network intrusion~~ conditions that collectively define known intrusion network security properties, wherein the second subset of templates comprises:

Operating System, Protocol, Application, Port, Length, Offset, Threshold, Contains, ContainsHex, Flags, FragmentID, IcmpType, IcmpCode, PayloadSize, and TimeToLive.

7. (Currently amended) The method of claim 1, wherein the step of constructing query-based rules includes associating each rule with an operating system of at least one network resource.

8. (Currently amended) A method for use in analyzing network security, comprising:

constructing rules to be used ~~to identify network conditions, including vulnerability conditions and intrusion conditions~~ for determining the presence of a set of conditions in at least one network resource, wherein the set of conditions collectively define known network security properties of the at least one network resource in which the set of conditions are present, wherein the known network security properties include known vulnerability network security properties and known intrusion network security properties, the rules constructed from a set of lexical elements that include a set of templates,

where each rule for identifying a vulnerability condition is associated with an operating system.

9. (Original) The method of claim 8, wherein the set of lexical elements further includes a set of statements and a set of reserved words.

10. (Original) The method of claim 8, wherein the templates in the set of templates are classified in one of two classes comprising template types and template actions.

11. (Cancel)

12. (Cancel)

13. (Currently amended) A vulnerability detection system comprising:

a rule constructor that allows a user to construct rules based on specified lexical elements, where the rules are to be used ~~to identify vulnerability conditions~~ for determining the presence of a set of conditions in at least one network resource, wherein the set of conditions collectively define known network security properties of the at least one network resource in which the set of conditions are present ~~in a network.~~

14. (Original) The vulnerability detection system of claim 13, wherein the lexical elements include a set of statements, a set of templates, and a set of reserved words.

15. (Original) The vulnerability detection system of claim 13, wherein:

the rule constructor includes a graphical user interface to receive information from a user constructing a rule; and

the rule, once constructed, is stored in a rule database.

16. (Original) The vulnerability detection system of claim 13, wherein the rule constructor requires each rule to be associated with an operating system.

17. (Currently amended) A system for use in network security, comprising:

a rule constructor that allows a user to construct rules based on specified lexical elements, where the rules are to be used ~~to identify vulnerability conditions~~ for determining the presence of a set of conditions in at least one network resource, wherein the set of conditions collectively define known network security properties of the at least one network resource in which the set of conditions are present, wherein the known network security properties include known vulnerability properties ~~in a network~~;

a database for storing the rules; and

a vulnerability detector designed to gather information about a network and to use that information along with the stored rules to determine if a vulnerability ~~condition~~ exists on at least one network resource of the network based on the known vulnerability properties of the network resource.

18. (Currently amended) A vulnerability detection system, comprising:

a rule database that includes rules that are based on specified lexical elements, including a set of templates, wherein the rules are to be used for determining the presence of a set of conditions in at least one network resource, wherein the set of conditions collectively define known vulnerability properties of the at least one network resource in which the set of conditions are present ~~to identify vulnerability conditions on a network~~.

19. (Original) The vulnerability detection system of claim 18, wherein the lexical elements further include a set of statements and a set of reserved words.

20. (Original) The vulnerability detection system of claim 18, wherein each rule is associated with a specified operating system.

21. (Currently amended) An intrusion detection system comprising:

a rule constructor that allows a user to construct rules based on specified lexical elements, where the rules are to be used for determining the presence of a set

of conditions in at least one network resource, wherein the set of conditions collectively define known intrusion properties of the at least one network resource in which the set of conditions are present ~~to identify intrusion conditions in a network~~.

22. (Original) The intrusion detection system of claim 21, wherein the lexical elements include a set of statements, a set of templates, and a set of reserved words.

23. (Original) The intrusion detection system of claim 21, wherein:

the rule constructor includes a graphical user interface to receive information from a user constructing a rule; and

the rule, once constructed, is stored in a rule database.

24. (Currently amended) A system for use in network security, comprising:

a rule constructor that allows a user to construct rules based on specified lexical elements, where the rules are to be used ~~to identify intrusion conditions~~ for determining the presence of a set of conditions in at least one network resource, wherein the set of conditions collectively define known network security properties of the at least one network resource in which the set of conditions are present ~~in a network~~;

a database for storing the rules; and

an intrusion detector designed to monitor network traffic and to check that network traffic against the stored rules to determine if an intrusion ~~condition~~ exists on the network, the intrusion detector further designed to notify a user of the presence of an intrusion ~~condition~~ in at least one network resource, but only if the intrusion ~~condition~~ is applicable to the network resource based on the known intrusion properties of the network resource.

25. (Currently amended) An intrusion detection system, comprising:

a rule database that includes rules that are based on specified lexical elements, including a set of templates, wherein the rules are to be used ~~to identify intrusion conditions~~ for determining the presence of a set of conditions in at

least one network resource, wherein the set of conditions collectively define known network security properties of the at least one network resource in which the set of conditions are present ~~on a network~~.

26. (Original) The intrusion detection system of claim 25, wherein the lexical elements further include a set of statements and a set of reserved words.

27. (Currently amended) A computer readable medium on which is stored a set of instructions, which when executed, cause the performance of the following steps:

storing a set of rules to be used ~~to identify vulnerability conditions and intrusion conditions~~ for determining the presence of a set of conditions in at least one network resource, wherein the set of conditions collectively define known network security properties of the at least one network resource in which the set of conditions are present, wherein the known network security properties include known vulnerability properties and known intrusion properties, which rules are constructed from a set of lexical elements that include a set of templates, where ~~each~~ at least a subset of rules of the set of rules ~~for identifying a vulnerability condition~~ is associated with an operating system.

28. (Original) The method of claim 27, wherein the set of lexical elements further includes a set of statements and a set of reserved words.

29. (Original) The method of claim 27, wherein the templates in the set of templates are classified in one of two classes comprising template types and template actions.